UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

EPIC SYSTEMS CORPORATION, a Wisconsin Corporation,

Plaintiff,

v.

TATA CONSULTANCY SERVICES LIMITED, an Indian Corporation; and TATA AMERICA INTERNATIONAL CORPORATION (dba TCS AMERICA), a New York Corporation,

Defendants.

Case No. 14-CV-748

DEMAND FOR JURY TRIAL

SECOND AMENDED COMPLAINT

Tata Group is one of the largest companies in the world. It is a private conglomerate headquartered in Mumbai, India, with worldwide reach, achieving revenues last year of $103 billion. One of Tata Group's largest subsidiaries is Tata Consultancy Services, also headquartered in Mumbai, India. Like Tata Group, Tata Consultancy Services is a worldwide behemoth in its own right, providing information technology and services through more than 300,000 employees and generating nearly $13.5 billion in annual revenues. Founded by a division of Tata Sons Limited in 1968, Tata Consultancy Services is itself the largest public Indian company, as measured by market capitalization, and is the largest India-based information technology services company, as measured by revenues.

As President Obama recently articulated during the State of the Union Address, it is a matter of great national concern that "[n]o foreign nation, no hacker, should be able to . . . steal our trade secrets." Yet Tata Consultancy Services has done just that, brazenly stealing the trade

secrets, confidential information, documents, and data of a privately held healthcare software company in Wisconsin called Epic Systems Corporation. The theft appears to have been masterminded in Mumbai, then carried out in both India and the United States through employees of a U.S. subsidiary of Tata Consultancy Services called Tata America International Corporation. The theft was accomplished by fraudulently and illegally gaining access to Epic's computer systems through the Internet. This lawsuit is the result of that theft.

In particular, Plaintiff Epic Systems Corporation ("Epic") complains against Defendants Tata Consultancy Services Limited ("TCS India"), and Tata America International Corporation (dba "TCS America"), as follows:

NATURE OF THE CASE

1. Epic seeks damages and injunctive relief to prevent TCS India and TCS America (collectively "TCS"), and potentially other Tata-related entities such as Tata Group and Tata Sons Limited, from disclosing or misusing documents, data, confidential information, trade secrets, and other valuable information and intellectual property stolen from Epic. The misuse and disclosure of valuable Epic property flows from a series of computer fraud and computer theft violations by TCS personnel in the United States and India.

2. Epic is a Verona, Wisconsin based healthcare company that makes software for mid-size and large medical groups, hospitals, and integrated healthcare organizations. Epic works with customers that include community hospitals, academic facilities, children's organizations, safety net providers, and multi-hospital systems. Epic's integrated software spans clinical, access, revenue, and managed care plan functionality. Epic's software manages the collection and storage of patient data and care process data into a common database, including records of patient admissions and discharges, pharmacy, specialty care, billing, insurance

benefits, and referral information. Epic's software is used by an estimated 281,000 physicians worldwide to manage the care and records of an estimated 169 million patients. The company and its high quality, integrated software products are recognized leaders in the healthcare software industry.

3. Epic is a privately held company. It has internally developed, installed, and supported its applications since its inception in 1979. The know-how and development of Epic's software is the result of careful, hard work by its employees at a tremendous monetary cost and expenditure of man-hours over a period of decades.

4. Epic's intellectual property, confidential information, documents, and trade secrets are of the utmost importance to Epic and the company takes reasonable means to protect those assets. Epic shares its confidential information and trade secrets on a need-to-know basis with its employees and certain customers subject to confidentiality obligations designed to protect Epic's computer network, software, documents, confidential information, and trade secrets. Epic regularly requires parties with which it does business to execute written non-disclosure agreements. Epic utilizes processes and tools to monitor whether its materials are publicly disclosed, and has processes in place to review materials before publication from its customers.

5. Epic maintains its confidential business information on its computer systems that can be accessed only by authorized users. Epic does allow third parties (such as customers and consultants working for customers) to access some information through Epic's UserWeb web portal if necessary to further implementation, integration, or testing of Epic's software at a customer facility. To gain access credentials to enter into Epic's UserWeb web portal, a person must contact and register with Epic, agree to strictly protect Epic's confidential information, and

agree not to use the Epic information in a manner harmful to Epic. Those outside Epic are not able to access Epic's UserWeb to access or download data unless they have registered with Epic as a customer or a consultant who is supporting an Epic customer.

6. Despite Epic's precautions, and promises from TCS not to wrongfully disclose or misuse Epic's confidential information but only to use it for the purpose of supporting Epic's customer, TCS personnel wrongfully accessed Epic's UserWeb and downloaded a substantial amount of data containing Epic documents, confidential information, trade secrets, and other valuable assets owned by Epic. In fact, it appears that much of the stolen data was not even required for the TCS personnel who downloaded the files to provide consulting services to Epic's customer. Significantly, much of the data wrongfully taken from Epic, if used improperly, would provide an unfair development and design advantage for TCS's competing medical management software called Med Mantra.

7. Rather than compete lawfully with Epic, TCS has engaged in what appears to be an elaborate campaign of deception to steal documents, confidential information, trade secrets, and other information and data from Epic, for the purpose of realizing technical expertise developed by Epic over years of hard work and investment. TCS's misconduct appears designed to allow TCS and perhaps other Tata entities to unfairly compete with Epic in the U.S. and global marketplace. The unlawful conduct of TCS and potentially other Tata entities must be stopped and an appropriate remedy fashioned for the benefit of Epic.

THE PARTIES

8. Plaintiff Epic is a Wisconsin corporation with its principal place of business located at 1979 Milky Way in Verona, Wisconsin. Epic is a leading developer and distributor of software products for the healthcare industry. Epic markets and licenses software products,

including electronic medical records software, for use in the healthcare industry throughout the United States and the world.

9. Defendant Tata Consultancy Services Limited ("TCS India") is an Indian Corporation with its principal place of business located in Mumbai, India. The company specializes in information technology services, consulting, and business solutions, and does over half of its business in the Americas. TCS India also develops and markets software products, including the hospital management system Med Mantra, which is discussed in detail at the TCS website: http://www.tcs.com/SiteCollectionDocuments/Brochures/Healthcare_Brochure_Med-Mantra-Healthcare-Solution_0612-1.pdf. TCS India markets Med Mantra as providing "Patient Health Management through EMR [Electronic Medical Record]," which "together with strong clinical functionality makes for a comprehensive solution" for hospitals. Med Mantra is being designed by TCS, and perhaps other Tata entities, to directly compete with Epic software products. Indeed, TCS India markets Med Mantra to be compliant with a number of international healthcare standards "such as HL7, ICD 10, ICD 9CM, LOINC, HIPAA and many more," which include standards applicable to the United States. http://www.tcs.com/industries/healthcare/Pages/Med-Mantra-Hospital-Management-Solution.aspx.

10. Defendant Tata America International Corporation (dba "TCS America") is a New York corporation with its principal place of business located at 101 Park Avenue, Suite 2603, New York, New York 10178. TCS America appears to be a wholly-owned subsidiary of TCS India and is registered to do business in Wisconsin.

11. At all times mentioned herein, TCS India and TCS America were the agents of one another, acting in the full course and scope of said agency. In addition, on information and

belief, at all times mentioned herein, TCS India and TCS America were the alter egos of each other. A unity of interest in ownership and other interests between TCS India and TCS America existed such that any separateness ceased to exist between them, and each was the mere instrumentality of the other. For example, TCS India and TCS America operate under the same name (both regularly do business as "TCS"); use the same logo for their businesses; maintain interconnected websites that link to each other, with the TCS India website including a separate page for TCS America; and use the same email protocol. The companies appear to also use the same computer network and other shared services. Both TCS entities have the same principal executive office in the United States, have the same registered agents in the states in which they are both registered to do business, and have overlapping leadership. They share the same legal counsel and have acted as a single entity thus far in this matter, submitting joint briefs and speaking with a single voice. Furthermore, both TCS entities offer the same services and products, with TCS America merely acting as the North America operation of TCS India.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1367(a) and 18 U.S.C. § 1030. This action involves the Defendants' violations of the Computer Fraud and Abuse Act, and related misconduct.

13. This Court alternatively has jurisdiction pursuant to 28 U.S.C. § 1332(a). The dispute arises between citizens of different states (Epic is a citizen of Wisconsin, TCS America is a citizen of New York) and a citizen of a foreign state is an additional party (TCS India is a citizen of India) and the amount in controversy exceeds the sum of $75,000, exclusive of interests and costs.

14. TCS America and TCS India are subject to personal jurisdiction in Wisconsin. TCS America is registered in and authorized to conduct business in Wisconsin, and has a registered agent located in Madison, Wisconsin. TCS India and TCS America also directed their tortious and illegal conduct at Wisconsin, stealing documents and information from Wisconsin; wrongfully accessed servers physically located in Wisconsin; and knowingly caused related losses, damages, and injuries to Epic in Wisconsin. The Defendants are engaged in substantial business activities within Wisconsin. They are, and were at the time of the injury, engaged in solicitation and service activities in Wisconsin, and materials and things manufactured, serviced, and processed by the Defendants are used and consumed in Wisconsin. TCS America also entered into a Standard Consultant Agreement with Epic, under which TCS America consented to personal jurisdiction of the state and federal courts located in Wisconsin.

15. Venue is proper in the United States District Court for the Western District of Wisconsin pursuant to 28 U.S.C. §§ 1391 and 1400 because TCS America or its agent may be found in this judicial district, TCS India and TCS America are subject to personal jurisdiction in this judicial district, and a substantial portion of the events giving rise to this action occurred within this district. The servers wrongfully accessed and from which information and documents were stolen are physically present in this district. Furthermore, the intellectual property and confidential and proprietary information that is the subject of these allegations was created in and is situated in this judicial district.

FACTUAL BACKGROUND

Epic's Licensing Agreement With Kaiser

16. Kaiser Permanente is the largest managed healthcare organization in the United States. In 2003, Kaiser Permanente chose Epic to manage its enormous records system. Kaiser

Permanente is comprised of three distinct groups, one of which is Kaiser Foundation Hospitals ("Kaiser"). Kaiser is a substantial customer and user of Epic software. On February 4, 2003, Epic entered into a written agreement with Kaiser (the "Kaiser Agreement") under which Epic agreed to license certain computer software to Kaiser to support patient care delivery activities at all of Kaiser's venues.

17. Pursuant to the Kaiser Agreement, Epic has provided Kaiser with access to Epic's UserWeb, a protected electronic workspace through which Epic provides training and other user materials, such as program manuals, to assist customers with their implementation and maintenance of Epic products. The Kaiser Agreement also contains provisions protecting Epic's confidential information by allowing dissemination of information only to persons with a need to know. It also contains restrictions on the use of the Epic confidential information, limiting the uses to those needed to fulfill the purpose of the Kaiser Agreement.

18. Healthcare organizations regularly hire third party software analysts, software test engineers, and other technology consultants to support their computer networks and their employees' ability to use the networks. These consultants assist in the installation, configuration, operation, and support of Epic's electronic medical records systems at various Epic customers. In some cases these consultants are engaged to alter customer systems to improve system compatibility and train employees of Epic's customers.

19. Access to the Epic UserWeb is limited to those who require access to Epic information in order to facilitate installation, maintenance, or support of Epic software in use by a particular customer of Epic. Each user who attempts to access the Epic UserWeb must complete an online registration form. The registration includes a UserWeb log-in and password.

20. The UserWeb registration form requires each registrant to provide his or her employer information, including whether the registrant is an "employee of an Epic customer," or a "consultant" for an Epic customer. Employees of Epic customers are granted access to the Epic UserWeb without additional restrictions because the customer has already contractually promised not to wrongfully use or disclose Epic documents or information (ordinarily in a detailed written agreement governing the entire relationship between Epic, its products, and the customer).

21. Consultants who have been hired by customers, on the other hand, are required to complete a UserWeb Access Agreement before their account can be considered for approval and authorization for access granted by Epic. The agreement is designed to provide a layer of protection for Epic before the consultants, some of whom work for companies that compete with Epic, may access Epic's UserWeb. The UserWeb Access Agreement includes the following provisions, among others: (1) it prohibits consultants from granting access to or allowing any third party to use the UserWeb password issued to them or access the UserWeb; (2) it requires consultants to "maintain in confidence all Confidential Information and not disclose it to others," except "to the extent necessary for performance of the Project;" and (3) it prohibits consultants from using Epic's confidential information "for any purpose other than performance of the Project," including to "[r]everse engineer any Epic or third party software located or described on the UserWeb or any part thereof."

22. In addition, under the UserWeb Access Agreement, consultants are not eligible to obtain access to the UserWeb until their consulting firm has entered a Consultant Access Agreement with Epic for the applicable customer. The specifics of the Consultant Access Agreement are designed to limit the Consultant's use of information and protect Epic from any

improper use or disclosure of its software, documents, trade secrets, confidential information, intellectual property, or the other valuable information on the Epic UserWeb.

23. Even if a consultant is granted access to the UserWeb, that access is more limited than the access granted to Epic's customers. Epic purposefully circumscribes consultants' access to a limited area that is necessary for the consultant to support the customer. The UserWeb Access Agreement obligates the "User" who agrees to the agreement to accept access to UserWeb only for purposes of performing the specific services for or on behalf of the Epic customer. Each consultant User agrees that he or she will not share the login password with any other person, or grant access for any other person to login to UserWeb. The User further agrees that he or she will not use the Epic confidential information for any purpose other than performance of the Customer project that the consultant is supporting.

24. Epic requires the UserWeb Access Agreement and agreements with consulting firms to protect its documents, confidential information, trade secrets, and other intellectual property, and to take reasonable steps to prevent unauthorized disclosure or use of the intellectual property assets of Epic. Consultants are not authorized to access the Epic UserWeb without agreeing to the UserWeb Access Agreement. Their authorization is expressly limited by the terms of that agreement.

Epic's Standard Consultant Agreement with TCS

25. TCS is not an Epic customer. Rather, it provides consulting services to Epic's customers. TCS is also a competitor of Epic in that it is offering competing software systems and services.

26. In August 2005, in connection with Epic's ongoing provision of computer software services to Kaiser, several individuals claiming to be Kaiser employees registered with

Epic to receive certain software training classes. When Epic personnel realized that the registering individuals' email addresses were from TCS, not Kaiser, they immediately contacted Kaiser regarding the discrepancy. Kaiser responded that the individuals were in fact TCS employees consulting for Kaiser, apparently working with Kaiser in support of its complex computer networks and software systems. Epic physically removed the TCS employees from the Epic training course and informed them that TCS personnel could not take the course until Epic received an executed non-disclosure agreement from TCS.

27. Shortly thereafter, on August 10, 2005, Epic and TCS America entered a Standard Consultant Agreement (the "TCS America Agreement") whereby Epic agreed to allow certain TCS employees access to Epic training programs for purposes of providing consulting services to Epic's customers related to the implementation of "Epic Program Property."

28. The TCS America Agreement defines Epic Program Property to be the "computer program object and source code and the Documentation for all of Epic's computer programs." In the TCS America Agreement, TCS agreed that Epic's Program Property "contains trade secrets of Epic protected by operation of law and this Agreement."

29. The TCS America Agreement included confidentiality provisions and use restrictions whereby TCS agreed that it, its employees, and its agents would do the following, among other things, to protect Epic's rights:

a. TCS will "limit access to the Program Property to those [TCS employees] who must have access to the Program Property in order to implement the Program Property on Epic's or its customer's behalf" (i.e., Kaiser);

b. TCS will not "use the Program Property … for any other purpose other than in-house training of [TCS] employees to assist Epic customers in the implementation of the Program Property licensed by that Epic customer;"

c. TCS will "require any [TCS] employees who are given access to the Confidential Information to execute a written agreement … requiring non-disclosure of the Confidential Information and limiting the use of the Confidential Information to uses within the scope of the employee's duties conduct pursuant to this Agreement" or "inform all such employees that [TCS is] obligated to keep Confidential Information confidential…" ("Confidential Information" is defined as information "concerning the functioning, operation or Code of the Program Property, Epic's training or implementation methodologies or procedures, or Epic's planned products or services");

d. TCS will "use Confidential Information only for the purpose of implementing the Program Property on an Epic customer's behalf;"

e. TCS will "notify Epic promptly and fully in writing of any person, corporation or other entity that You know has copied or obtained possession of or access to any of the Program Property without authorization from Epic;" and

f. TCS will not permit any employee who has had access to the Program Property to participate in any "development, enhancement or design of, or to consult, directly or indirectly, with any person concerning any development, enhancement or design of, any software that competes with or is being developed to compete with Epic Program Property…."

30. The TCS America Agreement covered the work of TCS consultants at Kaiser. Although Epic terminated the TCS America Agreement shortly after filing this lawsuit, the

confidentiality and use restrictions articulated in the agreement remain in effect "for the maximum duration and scope allowed by law."

31. On information and belief, since 2005 the Defendants have continued to provide consulting services to Kaiser related to the implementation and maintenance of Epic Program Property.

32. TCS India and/or TCS America are currently or until recently were performing a Testing Center of Excellence contract with Kaiser, under which TCS personnel have developed and implemented processes, tools, and best practices for testing and improving certain Epic Program Property licensed to Kaiser under the Kaiser Agreement.

TCS's Unauthorized Access, Fraud, and Theft of Epic Information

33. Prior to initiating this action, Epic learned from an informant, TCS employee Philippe Guionnet, that TCS personnel have been fraudulently and without authorization accessing Epic's UserWeb computer network, and that the information obtained through the unauthorized access into UserWeb was being used by TCS to benefit its competing Med Mantra software. In his capacity at TCS, Mr. Guionnet was responsible for managing all aspects of TCS's contract with Kaiser to provide consulting services and reported directly to TCS executive management.

34. According to Mr. Guionnet, TCS leaders in the U.S. and India were aware of and complicit in TCS's scheme to unlawfully gain unauthorized access to Epic's UserWeb and information and misuse confidential Epic information and valuable intellectual property for the benefit of TCS. The unauthorized access by TCS began as early as 2012.

35. Mr. Guionnet further described that an access credential for the UserWeb has been used by Defendants in India to access Epic's UserWeb without authorization to download

information from Epic's UserWeb, including Program Property and Confidential Information within the meaning of the TCS America Agreement, and that the purpose of the misconduct was to use information and documents related to Epic's leading software to benefit TCS's creation of and improvements to TCS's competing Med Mantra product.

36. After learning of the unauthorized and illegal downloading of Epic information by TCS personnel, and the apparent purpose of the misconduct, Epic investigated its protected UserWeb and discovered that an account associated with Ramesh Gajaram, a TCS employee who worked as a consultant for Kaiser in Portland, Oregon, and who worked on projects related to Epic's provision of software and services to Kaiser, had downloaded from Epic's UserWeb at least ***6,477 documents*** accounting for ***1,687 unique files***. These documents included Program Property and Confidential Information within the meaning of the TCS America Agreement.

37. The access credentials of Mr. Gajaram were used to access the Epic UserWeb from an IP address in India during the time when Mr. Gajaram worked in Portland, Oregon. The access credentials were also utilized from other IP addresses around the United States, outside of Oregon, during that same time period. Furthermore, Epic determined that Mr. Gajaram's credentials were used to download documents from IP addresses in India registered to TCS—meaning that someone else within TCS, but outside the Kaiser network, used Mr. Gajaram's login credentials as if they were Mr. Gajaram. This evidence uncovered by Epic appears to confirm much of Mr. Guionnet's information regarding TCS's misconduct.

38. Mr. Gajaram transferred his access credentials to at least two other TCS employees, Aswin Kumar Anandhan and Sankari Gunasekaram. Upon information and belief, at the time of the transfer, Mr. Gajaram was located in the United States and Mr. Anandhan and Mr. Gunasekaram were located in India. Neither Mr. Anandhan nor Mr. Gunasekaram were

authorized to use those credentials or had received permission or any authorization to take Epic information from Epic's UserWeb, and neither needed the information in connection with the implementation of Epic's Program Property for Kaiser.

39. Epic is still investigating the specific stolen documents, but the documents downloaded by TCS personnel included, among other things, confidential, proprietary, and trade secret documents detailing over twenty years of development of Epic's proprietary software and database systems, including programming rules and processes developed to produce optimal functionality of Epic's software; documents that decode the operation of its source code that would otherwise be unusable to those outside of Epic; and information regarding Epic's system capabilities and functions, including procedures for transferring data between customer environments, rules related to information collection, methods for limiting access to patient records, and processes for converting customer data, all of which reveal decades of Epic's work with its customers to determine the functionality desirable or required for Epic to provide successful products to those customers.

40. Further, it appears that many of these downloaded Epic documents were not even required for Mr. Gajaram to perform his own job functions in support of Kaiser. For example, the downloaded Epic documents include a guide containing confidential and/or trade secret information that provides a blueprint for understanding Epic's source code or competing with Epic's infrastructure.

41. In addition to the enormous number of downloads accomplished through the misuse of Mr. Gajaram's UserWeb log-in credentials, it was discovered that the credentials had been obtained by Mr. Gajaram and TCS in a fraudulent manner. When Mr. Gajaram registered for his credentials, he misrepresented that he was a "customer employee" instead of a

"consultant," even though Epic requires consultants to specifically identify themselves as such. He also used a kp.org email address, which Kaiser provides to its consultants for use while consulting for Kaiser, to further mislead Epic into believing that Mr. Gajaram was an employee of Kaiser when he was in fact an employee of TCS.

42. Mr. Gajaram appears to have intentionally misrepresented himself as a Kaiser employee, when he knew his representation was false, for the purpose of avoiding the restrictions of the UserWeb Access Agreement that apply to consultants and gaining customer-level access authorization to Epic's UserWeb. Mr. Gajaram was never properly authorized to have customer level access and only gained that access through misrepresentation. By gaining customer-level access, rather than consultant access, as a TCS employee Mr. Gajaram exceeded the access granted by Epic to TCS personnel for the express purpose of implementing, integrating, or testing Epic's software at Kaiser.

43. Upon discovery of the fraudulent access to and excessive downloading from the Epic UserWeb by Mr. Gajaram, Epic suspended Mr. Gajaram's User ID so that no further access or downloading could occur.

44. Shortly thereafter, Mr. Gajaram sought via email to have his access to the UserWeb reactivated so that he could again gain access to the UserWeb. He sent two emails on June 24, 2014, and June 30, 2014, seeking reactivation of his account. The first email on June 24 included a signature line indicating that his title was "QA Lead, Kaiser Permanente." The second email on June 30 included a different signature line indicating that Mr. Gajaram was actually an "Onshore Test Lead" for TATA Consultancy Services as well a "QA Lead" title for Kaiser. On information and belief, the first email deleted the identification of TATA Consultancy Services so as to mask the fact that Mr. Gajaram was not with Kaiser but rather

TCS. Mr. Gajaram also appears to have understood that the access he sought exceeded access that would be granted to a consultant, and appears to have tried multiple times to regain his access knowingly using different postures, once as a Kaiser employee and once as a TCS consultant.

45. There appears to be no legitimate reason for Mr. Gajaram and those he was conspiring with from TCS to download more than six thousand files from Epic, or to download some of the specific pieces of confidential data he targeted on the Epic system. Much of the information taken would not even have been needed by Mr. Gajaram to perform his limited job function supporting Kaiser, and certainly would not have been needed by Mr. Anandhan or Mr. Gunasekaram to perform their job duties. Certain documents downloaded by the TCS employees were not available to consultants for Kaiser. For example, Mr. Gajaram only gained access to confidential and/or trade secret documents such as the Community Connect Install Summary, ADT End-User Proficiency Question Bank, ED Registrar Checklist, and the Physician's Guide to EpicCare Ambulatory zip file (among many others) by fraudulently representing himself as a Kaiser employee.

A TCS Employee Admits To Wrongdoing

46. When confronted by Kaiser regarding this downloading of Epic data, Mr. Gajaram initially denied the downloading. He claimed that he only viewed Epic information on UserWeb, but did not save or download any Epic materials. In short, as TCS has done in this case, Mr. Gajaram initially denied any wrongdoing.

47. After being presented with the download logs associated with his account, Mr. Gajaram changed his story and admitted that he had provided his Epic access credentials to two other TCS personnel, in violation of the UserWeb Access Agreement. He also admitted that

these other TCS personnel did not need access to the Epic UserWeb to perform job functions in support of Kaiser.

Epic Uncovers More Misconduct By TCS Personnel

48. On July 29, 2014, Epic suspended the UserWeb access credentials for another TCS consultant working with Kaiser after it was determined that this additional TCS employee had also downloaded Epic documents which have no apparent relationship to the TCS employee's position as a consultant supporting Kaiser.

49. Epic is still investigating the misconduct of TCS personnel and does not yet know the extent of the damage caused by TCS's misconduct.

50. To date, Epic has incurred far more than $5,000 in costs and losses related to investigating Defendants' unauthorized access to Epic's UserWeb. Epic will continue to incur costs, losses, and damages as it seeks to uncover how much of its intellectual property, trade secrets, confidential information, internal documents, and other Epic information and data was taken by TCS personnel.

51. Details regarding the sensitive materials taken by TCS personnel cannot be disclosed in this publicly filed document but will be identified for the Court and the parties in this case, consistent with Epic's discovery obligations, after an appropriate protective order is entered to protect Epic's valuable information and intellectual property and TCS discloses for the Court and parties the extent of its misconduct. Epic has already provided TCS with a list of the thousands of documents taken from Epic.

52. Unless restrained by this Court, TCS's unauthorized access to Epic's intellectual property, trade secrets, confidential information, internal documents, and other information and data, and subsequent theft of Epic's intellectual property, trade secrets, confidential information,

internal documents, and other information and data by downloading from the UserWeb, will allow TCS to shortcut years of hard work and investment expended by Epic in developing Epic's industry-leading medical software products.

53. TCS's actions set forth above were malicious and taken with an intentional disregard of the rights of Epic.

The TCS Informant's Discovery Objections

54. After Epic initiated this action, TCS served a subpoena *duces tecum* on Mr. Guionnet, requesting documents and communications relating to the access and downloading of Epic information by TCS personnel.

55. On January 5, 2015, Mr. Guionnet responded with written objections to the subpoena, requesting that the subpoena be quashed or modified pursuant to Rule 45 of the Federal Rules of Civil Procedure. Mr. Guionnet subsequently responded with continued written objections to the subpoena, specifically disputing a number of prior statements made by TCS in this civil action concerning Mr. Guionnet and the conduct of TCS and its personnel.

56. In particular, Mr. Guionnet stated in his objections that he was a "Client Partner on the Kaiser Account" for TCS until May 2014. According to Mr. Guionnet, in that role, his duties included, among other things, making decisions on the account, holding and attending regular staff meetings and client meetings, travelling with the client to India and attending technical, sales, and marketing activities specific to the Kaiser account, and submitting financial forecasts on a weekly basis. Mr. Guionnet stated that he was also named an "identified leader in the organization."

57. Mr. Guionnet wrote in his objections that he was a "star employee, with exceptional performances," which was recognized in his April 2014 review. He disputed that he

was a "professional whistleblower," as TCS has characterized him in this action. To the contrary, Mr. Guionnet stated that he had provided multiple "opportunities to cure" to TCS management, including his Business Unit Head, Syama Sundar, and Division President, Suresh Muthuswami. Mr. Guionnet stated that he had also made requests to the Chief Financial Officer, President of TCS Americas, Chief Legal Officer, and certain TCS executives to be put in contact with the Audit Committee regarding the conduct of TCS.

58. With respect to MedMantra, Mr. Guionnet stated in his objections that it was "NOT TRUE that my job responsibility had nothing to do with MedMantra," and that he would be able to produce information that substantiates his position. He stated: "Resources associated with MedMantra are identifiable in multiple teams spread throughout the [TCS] organization and spread in multiple locations, either in development and programming, design, architecture, innovation, infrastructure, product development, security, operation, etc[.]"

59. According to Mr. Guionnet, a large portion of his team was called "Care Delivery (typically named for activities in Hospitals, clinical, lab, pharmacy, etc.)," and the scope included "TCOE/Epic Testing" and "Analytics off of Epic platform." His team "had a substantial dotted line to a Global Group also called Care Delivery (typically including Hospitals i.e. MedMantra, lab, ambulatory, etc.)," and "Operation & Delivery for Kaiser (including Epic support from India) ultimately reported to the same person in charge of Care Delivery." Mr. Guionnet stated: "It is fair to say that this individual in charge globally of MedMantra, Care Delivery, [and] Operations is intimately aware-and-involved inthe [sic] MedMantra situation, intimately aware-and-involved in the Care Delivery activities at Kaiser and his group, intimately aware-and-involved of the Operation & Delivery activities at Kaiser and in his group and intimately aware-and-involved of the Medmantra [sic] environment."

60. As part of his job responsibilities, Mr. Guionnet further stated:

- "I was exposed to various MedMantra products and services multiple times."
- "I was exposed to another product called MedMantra, implemented at the Cancer Hospital in Kolkata; I met the person in charge of MedMantra there and was able to understand that the architecture, functionality, language, design, etc were drastically different from the MedMantra publicized to be at Apollo Hospitals."
- "I met the CIO (and several of his staff) at Apollo hospitals during a MedMantra presentation."
- "I met the person in charge at TCS of the MedMantra development & programming; that seemed to be, again, another version of MedMantra with a different content and different meaning as the other 2 above[]."

61. Mr. Guionnet disputed TCS's contentions in this case that MedMantra had been developed prior to TCS's wrongful access to and downloading of Epic's sensitive, confidential, and trade secret information, stating "I was able to identify that significant MedMantra components, including Ambulatory and Laboratory, were written/tested in 2013 and 2014."

62. Mr. Guionnet also disputed TCS's contention in this case that MedMantra and Epic are not competitors. Mr. Guionnet stated that "MedMantra, and the various meanings it contains, including peripheral products and accelerators, is a modular entity…which goes 'beyond hospital automation', including elements of 'transformation in patient care, resource management and information management' and is available in a 'Global Network Delivery Model'." With respect to development of MedMantra, Mr. Guionnet stated: "Regulatory and Hospital requirements have been notoriously a source of obstacle, frustration and costs to

MedMantra/TCS to enter the US market as a whole, they have been allegedly a 'source of interest,'" and some of the confidential information that TCS took from Epic contains information regarding "how they are handled at Kaiser in the Epic system…." He also stated that TCS and/or MedMantra potentially compete in several fashions, including, but not limited to:

- "[A]s a whole product;"
- "[A]s a trimmed version of the whole product (i.e. in a less-critical hospital environment);"
- "[A]t a modular level (i.e. ambulatory);"
- "[A]t existing clients like Kaiser in integration and additional services;"
- "[A]t existing clients like Kaiser for future opportunities of new products/services (i.e. Claims integration, future Membership functionality already discussed);"
- "[I]n solution accelerators;"
- "[I]n clinical functionality;" and
- "[I]n Ambulance/Ambulatory functionalities."

63. Further, Mr. Guionnet disclosed evidence that TCS has been marketing MedMantra products to Kaiser:

- "I was asked to share with Kaiser information from Apollo hospitals and related to MedMantra[.]"
- "I was asked to identify if there would be a partnership available with Kaiser and a pilot program available to implement MedMantra at Kaiser (i.e. not in a typical hospital with critical risks but rather a small clinical environment)."

- "I participated in a MedMantra presentation to Kaiser."
- "I was asked to identify if some MedMantra modules would fit at Kaiser."
- "I specifically reviewed some MedMantra functionalities and modules as an option to be implemented as Kaiser."
- "I specifically reviewed at length some MedMantra functionalities and modules in Laboratory as an option to be implemented at Kaiser."

64. Mr. Guionnet also confirmed that he "saw, and/or suspected, and/or was aware of several comparisons between MedMantra and Epic softwares, including by the MedMantra team."

65. With respect to TCS's access to Epic's sensitive, confidential, and trade secret documents on the UserWeb, Mr. Guionnet stated that it was "well known," including by "programmers, managers, engagement managers, client partners, business unit heads, President, head of Delivery, head of MedMantra & Global Care Delivery, head of testing services," that "the restricted access to the Epic portal was not authorized…."

66. Mr. Guionnet also stated that "multiple contacts to epic were made (i.e. to their onsite representative), including by our President, in order to negotiate with Epic some flexibility; some representation[s] of 'progress with the Epic relationship' were made to Kaiser who was growing uncomfortable." According to Mr. Guionnet, he sent several emails regarding the "fraudulent aspect of the situation," including to President Suresh Muthuswami, about the "potential risk to the Business Unit" and "potential risk he was creating for TCS as a whole."

67. Mr. Guionnet also stated that a member of the Med Mantra "development and programming team was 'embedded'" in Mr. Guionnet's Kaiser team, and that person's presence

was "suspicious, questionable and questioned." Mr. Guionnet stated that he was asked to "reintegrate" the embedded employee after removing that person from his team.

68. In reference to the TCS employees who accessed Epic's UserWeb, Mr. Guionnet stated in his written objections that "Mr Gajaram was caught with a fraudulent access but nevertheless attempted to obtain a fraudulent access afterwards, and was caught again. Besides Mr. Gajaram, another access was obtained fraudulently after I had left the Kaiser account, with full knowledge of Management."

69. Epic is still investigating Mr. Guionnet's statements, and discovery is ongoing. However, Epic's investigation to date has revealed facts consistent with Mr. Guionnet's statements in his objections to TCS's subpoena and inconsistent with TCS's broad claims in this case that it has done nothing wrong.

FIRST CAUSE OF ACTION

Computer Fraud and Abuse Act under 18 U.S.C. § 1030

(against All Defendants)

70. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 69 above.

71. Epic's computer system is a protected computer as that term is defined by the Computer Fraud and Abuse Act ("CFAA"). Defendants accessed Epic's UserWeb, without authorization and by exceeding their authorization, to obtain confidential business information and/or trade secrets belonging to Epic, and to engage in and advance a theft, including falsely claiming to be a Kaiser employee for the purpose of gaining access to information restricted to Epic customers, in violation of subsection (a)(2)(C) of the CFAA, 18 U.S.C. § 1030. Defendants also appear to have wrongfully and intentionally trafficked in passwords, distributing to a

number of people around the world confidential Epic UserWeb log-in credentials wrongfully obtained by TCS personnel, in violation of subsection (a)(6) of the CFAA. The conduct of TCS described above was knowing and intentional.

72. The actions of Defendants were without Epic's knowledge, permission, or authorization.

73. The actions of the defendants crossed state lines, including conduct from Oregon, Wisconsin, and other states, and involved interstate commerce.

74. As a result of the violation by Defendants of the CFAA, Epic has suffered loss, injury, and damages far in excess of $5,000, and Epic will continue to be injured irreparably, while Defendants will be unjustly enriched. Epic's losses include, among other things, costs and expenses related to investigating and identifying TCS's unauthorized access to Epic's UserWeb and efforts to remedy the breach and prevent further misconduct. The specific amounts of the losses and damages suffered by Epic will be set forth at the trial of this matter.

SECOND CAUSE OF ACTION

Computer Crimes Act under Wis. Stat. § 943.70

(against All Defendants)

75. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 74 above.

76. Defendants willfully, knowingly, and without authorization accessed, copied, and took possession of electronic data and information belonging to Epic (i.e., Epic's property) from Epic's UserWeb, without Epic's consent and without lawful authority.

77. Defendants disclosed restricted access codes and other restricted access information to unauthorized persons.

78. The conduct of Defendants interfered with the right of Epic to possess such property and directly and proximately caused injury to Epic.

79. The actions of Defendants constitute a violation of the Computer Crimes Act ("CCA"), Wis. Stat. § 943.70.

80. As a direct and proximate result of the violation by Defendants of the CCA, Epic has suffered damages and loss in a manner which will be set forth at the trial of this matter.

81. Additionally, pursuant to Wis. Stat. § 943.70, Epic is entitled to an injunction to prevent further and continuing violations of this statute.

THIRD CAUSE OF ACTION

Misappropriation of Trade Secrets under Wis. Stat. § 134.90

(against All Defendants)

82. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 81 above.

83. Certain files that Defendants downloaded without authorization from Epic's UserWeb contain "trade secrets" within the meaning of Wis. Stat. § 134.90(1)(c).

84. The downloaded files contain data from which Epic derives economic value because it is not generally known and not readily ascertainable by proper means to Epic's competitors. Access to the data would permit TCS and other wrongdoers to shortcut years of hard work and investment expended by Epic in developing Epic's industry-leading medical software products.

85. Epic takes significant steps to maintain the secrecy of the downloaded files, including by restricting access to Epic customers and requiring others to sign non-disclosure agreements and other use restriction agreements. Epic also uses physical and technological

restrictions to protect its valuable trade secret information, as described partially in this Complaint.

86. Defendants misappropriated Epic's trade secrets in violation of Wis. Stat. § 134.90(2)(a), by knowingly acquiring the trade secrets by improper means, including by at least one TCS employee misrepresenting himself as a Kaiser employee in order to gain access to Epic's UserWeb and breaching TCS's obligations to maintain the confidentiality of Epic's information under the TCS America Agreement.

87. Upon information and belief, Defendants misappropriated the downloaded files for the purpose of utilizing Epic's trade secrets, which the company has developed through decades of work and significant expense, for purposes of developing TCS's formerly elementary Med Mantra software in order to compete directly with Epic. Defendants have also violated Wis. Stat. § 134.90(2)(b), by using Epic's trade secrets without Epic's consent, knowing that the trade secrets were acquired by improper means.

88. Pursuant to Wis. Stat. § 134.90(3), Epic is entitled to an injunction to prevent the misappropriation and misuse of its trade secrets.

89. While some of the injury being caused by Defendants' actions is irreparable pursuant to Wis. Stat. § 134.90(3), Epic has suffered also damages as a result of Defendants' misappropriation of Epic's trade secrets and it is entitled to recover such damages and/or disgorgement of any profits received by Defendants from their misappropriation of Epic's trade secrets pursuant to Wis. Stat. § 134.90(4). An award of exemplary and punitive damages is also appropriate in light of the misconduct of TCS outlined herein.

FOURTH CAUSE OF ACTION

Breach of Contract

(against All Defendants)

90. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 89 above.

91. The TCS America Agreement is a valid agreement under which TCS America, acting as the agent and alter ego of TCS India, made certain promises that, while consulting for Kaiser, TCS America would protect Epic's confidential and proprietary information, including by restricting access to the information, limiting its use to training and other consulting activities for Epic customers, and preventing use of the information to design, develop, or enhance a competing software product.

92. Epic has done all of the things required of Epic under the TCS America Agreement.

93. All conditions required under the TCS America Agreement for Defendants' performance were excused or have occurred, as detailed herein.

94. Defendants have breached the TCS America Agreement and failed to protect Epic's confidential and proprietary information by, among other things, improperly utilizing UserWeb access credentials through non-registered employees and employees who do not require access to consult for an Epic customer; downloading Epic's confidential and proprietary information — including Program Property, Confidential Information, and Documentation as defined in the TCS America Agreement — and then sending that information to India for purposes other than implementing the Program Property on Epic's or its customer's behalf; and using Epic's confidential and proprietary information — including Program Property,

Confidential Information, and Documentation — to develop and enhance Defendants' software designed to compete with Epic products.

95. Epic has incurred substantial damages—and will continue to incur such damages—as a direct and proximate result of Defendants' willful and material breaches and willful misconduct in an amount to be proven at trial. All of these damages were foreseeable as the consequences of Defendants' breaches as alleged herein. The amount of damages will be set forth in detail at the trial of this matter, after the extent of TCS's misconduct is discovered through this case. Epic is also entitled to an award of nominal damages and a declaration that Defendants breached the TCS America Agreement.

96. If Defendants are allowed to continue breaching the TCS America Agreement as described above, Epic will suffer irreparable harm for which it has no adequate legal remedy.

FIFTH CAUSE OF ACTION

Breach of the Covenant of Good Faith and Fair Dealing

(against All Defendants)

97. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 96 above.

98. The TCS America Agreement is a valid agreement under which TCS America, acting as the agent and alter ego of TCS India, made certain promises to protect Epic's confidential and proprietary information, including by restricting access to the information and limiting its use to training and other non-competitive activities.

99. Defendants owed Epic a duty of good faith and fair dealing implied from the TCS America Agreement. The TCS America Agreement contained an implied covenant of good faith

and fair dealing that, among other things, prohibited Defendants from engaging in the misappropriation and misuse described above.

100. Epic has done all of the things required of Epic under the TCS America Agreement.

101. Through the intentional and deceitful conduct alleged above, Defendants breached the covenant of good faith and fair dealing implied in the TCS America Agreement and denied Epic benefits due to Epic under the agreement. This conduct includes TCS's improper distribution of UserWeb access credentials to non-registered employees and employees who do not require access to consult for an Epic customer, its downloading of thousands of documents from UserWeb containing Epic's confidential and proprietary information — including Program Property, Confidential Information, and Documentation as defined in the TCS America Agreement — and its utilization of confidential and proprietary information to benefit Defendants' own software products.

102. Even assuming these actions did not violate the express terms of the TCS America Agreement, Defendants' conduct violated the spirit of the TCS America Agreement, and deprived Epic of the fruits of that contract, by accomplishing exactly what the agreement of the parties sought to prevent.

103. Epic has incurred substantial damages—and will continue to incur such damages—as a direct and proximate result of Defendants' willful and material breaches of the implied covenants of good faith and fair dealing, and willful misconduct, in an amount to be proven at trial. All of these damages were foreseeable as the consequences of Defendants' breaches as alleged herein.

104. If Defendants are allowed to continue breaching the covenant of good faith and fair dealing implied in the TCS America Agreement as described above, Epic will suffer irreparable harm for which it has no adequate legal remedy.

SIXTH CAUSE OF ACTION

Fraud

(against All Defendants)

105. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 104 above.

106. When TCS employees registered for access to Epic's system, agreeing to abide by the conditions that govern access to the system, at least one of them claimed to be a Kaiser employee for the purpose of avoiding the UserWeb Access Agreement and gaining customer-level access to the UserWeb. Other TCS employees repeatedly accessed Epic's computer network, claiming, through the use of fraudulently obtained log-in credentials, to be persons other than themselves, and thus misrepresenting that most basic information to Epic. If Epic had known the user credentials were fraudulently obtained, had been trafficked, or that the users were not who they purported to be, Epic would not have granted access to its computer network.

107. Defendants' representations were false, and Defendants knew the representation was false when they made it. The false representations were made intentionally to advance TCS's apparent scheme to steal confidential information, documents, intellectual property, and other information from Epic. The representations were also made to allow TCS to access Epic's computer network without following the proper channels that Epic had put in place for consultants like TCS.

108. Defendants intended that Epic rely on the false representations, and Epic did in fact rely on the representations in granting at least one TCS employee customer-level access to the UserWeb and in allowing other TCS employees to access the Epic system using fraudulently obtained log-in credentials.

109. Epic has incurred substantial damages—and will continue to incur such damages—as a direct and proximate result of Defendants' intentional misrepresentations. The amount of Epic's damages will be proven at trial.

110. Defendants' misconduct as described herein was intentional, malicious and specifically directed at causing harm to Epic, entitling Epic to an award of exemplary and punitive damages in an amount to be determined at the trial of this matter.

SEVENTH CAUSE OF ACTION

Conversion

(against All Defendants)

111. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 110 above.

112. This cause of action is based on Epic's confidential information that does not meet the statutory definition of a trade secret. *See Burbank Grease Servs., LLC v. Sokolowski*, 2006 WI 103, ¶ 33, 294 Wis. 2d 274, 717 N.W.2d 781.

113. Epic was the owner of information and documents stored on its UserWeb, which was wrongfully accessed by TCS personnel.

114. Defendants willfully took, controlled, interfered with, and/or deprived Epic of documents and information without Epic's consent and without lawful authority, including information and documents that do not comprise trade secrets. The specific identification of the

information wrongfully converted by TCS will be uncovered through the discovery process and as Epic continues its own evaluation of the data stolen from its UserWeb.

115. As a result of the conversion by Defendants of Epic's property, Epic has been and will continue to be injured irreparably and otherwise, while Defendants will be unjustly enriched. Moreover, Defendants' actions with respect to Epic's property have seriously interfered with Epic's right to possess the property, damaging Epic in an amount that will be evidenced at the trial of this matter.

116. Defendants' misconduct as described herein was intentional, malicious, and specifically directed at causing harm to Epic, entitling Epic to an award of exemplary and punitive damages.

EIGHTH CAUSE OF ACTION

Common Law Unfair Competition

(against All Defendants)

117. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 116 above.

118. This cause of action is based on Epic's confidential information that does not meet the statutory definition of a trade secret. *See Burbank Grease Servs., LLC v. Sokolowski*, 2006 WI 103, ¶ 33, 294 Wis. 2d 274, 717 N.W.2d 781.

119. Epic has invested substantial time, labor, and money in the creation and development of its data systems, software, documents, and information.

120. Without Epic's authorization, Defendants intentionally and wrongfully used, and will continue to use, Epic's stolen documents, password credentials, and information in unfair competition with Epic. This use is in direct competition with the services offered by Epic.

121. Defendants have gained an unfair advantage in their competition with Epic because Epic, not Defendants, expended the time, money, and energy to create and develop the documents and information stolen from Epic, as detailed above.

122. Epic has incurred substantial damages—and will continue to incur such damages—as a direct and proximate result of Defendants' misconduct described above. The amount of those damages will be set forth at the trial of this matter.

123. Defendants' misconduct as described herein was intentional, malicious, and specifically directed at causing harm to Epic, entitling Epic to an award of punitive damages.

NINTH CAUSE OF ACTION

Injury to Business under Wis. Stat. § 134.01

(against All Defendants)

124. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 123 above.

125. This cause of action is based on Epic's confidential information that does not meet the statutory definition of a trade secret. *See Burbank Grease Servs., LLC v. Sokolowski*, 2006 WI 103, ¶ 33, 294 Wis. 2d 274, 717 N.W.2d 781.

126. Defendants conspired and acted in concert together to misappropriate and misuse Epic's confidential and proprietary information for the purpose of willfully or maliciously injuring Epic's business via competitive harm to Epic's competing software product, including EpicCare Inpatient and EpicCare Ambulatory.

127. The actions of Defendants constitute a violation of Wis. Stat. § 134.01.

128. As a direct and proximate result of the violation by Defendants of Wis. Stat. § 134.01, Epic has suffered damages and loss in an amount which will be proven at the trial of this matter.

TENTH CAUSE OF ACTION

Property Damages or Loss under Wis. Stat. § 895.446

(against All Defendants)

129. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 128 above.

130. This cause of action is based on Epic's confidential information that does not meet the statutory definition of a trade secret. *See Burbank Grease Servs., LLC v. Sokolowski,* 2006 WI 103, ¶ 33, 294 Wis. 2d 274, 717 N.W.2d 781.

131. Without Epic's consent, Defendants intentionally took and all Defendants have used property belonging to Epic, including Epic documents and other property found on Epic's UserWeb, with the intent to deprive Epic permanently of the possession, use, and/or value of such property in violation of Wis. Stat. § 943.20.

132. As a direct and proximate result of Defendants' wrongful actions, Epic has suffered damage and loss. Pursuant to Wis. Stat. § 895.446, Epic is entitled to actual damages, including all costs of investigation and litigation. The amount of these damages will be evidenced at the trial of this matter.

ELEVENTH CAUSE OF ACTION

Unjust Enrichment

(against All Defendants)

133. Epic pleads this Cause of Action in the alternative to the Fourth Cause of Action for breach of contract.

134. Epic realleges and incorporates by reference herein each allegation contained in paragraphs 1 through 132 above.

135. This cause of action is based on Epic's confidential information that does not meet the statutory definition of a trade secret. *See Burbank Grease Servs., LLC v. Sokolowski,* 2006 WI 103, ¶ 33, 294 Wis. 2d 274, 717 N.W.2d 781.

136. Epic was, and is, entitled to the benefit of the data, documents, and information that was stored on its UserWeb.

137. With full knowledge of Epic's rights, Defendants unjustly obtained the benefit of Epic's property, as described herein, resulting in inequity and damage to Epic, as described in more detail above.

138. At all relevant times, Defendants appreciated or had full knowledge of the benefit of the data and information, and other things, which they stole from Epic.

139. Defendants have unjustly and wrongfully benefited, and continue to benefit, from their misappropriation and use of the property of Epic, to the detriment of Epic and against the fundamental principles of justice, equity, and good conscience. Under the circumstances described above, it is inequitable for Defendants to accept or retain the benefit of Epic's confidential and proprietary information.

140. Defendants were unjustly enriched and Epic was damaged in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Epic prays for relief and judgment as follows:

a. An order from the Court granting the parties immediate and expedited discovery in the matter;

b. Preliminary and permanent injunctive relief appropriately fashioned by the District Court to prevent further injury to Epic, and to prevent Defendants from further benefiting from their misconduct as alleged herein, including but not limited to injunctive relief:

i. requiring Defendants to cease any and all use of any document, information, or trade secret, taken from Epic in violation of law;

ii. requiring Defendants to not disclose to any party any document, information, or trade secret, taken from Epic in violation of law;

iii. requiring Defendants to immediately destroy and/or permanently delete (1) all copies of Epic documents and information in any form (electronic or hardcopy) including without limitation any trade secret and confidential information acquired from Epic; and (2) all copies of any materials in any form containing any, or derived from any, Epic trade secret or confidential information;

iv. requiring Defendants to provide a detailed accounting of its search for and destruction of the documents and information described in (iii) above, including providing a list of all documents or information destroyed or deleted.

v. preventing Defendants from any further unauthorized access, or access exceeding authorization, of any computer network or system of Epic, including, without limitation, the UserWeb;

vi. preventing Defendants from further improper use or disclosure of Epic's trade secrets or confidential information;

vii. preventing Defendants from further improper use or disclosure of unlawfully obtained Epic property that is not a trade secret or confidential information; and

viii. preventing Defendants from selling or offering to sell products that utilize, embody, or were developed or enhanced using Epic's trade secrets and/or confidential information or unlawfully obtained Epic property.

c. An award of the actual and consequential damages and loss that Epic has sustained as a result of Defendants' wrongdoing;

d. An award of nominal damages;

e. Disgorgement of Defendants' profits arising from the benefits of Defendant's use of Epic's confidential and proprietary information;

f. An award of all costs of investigation and litigation related to Epic's theft and misappropriation of Epic trade secrets and/or confidential information;

g. An award of punitive damages against Defendants in an amount to be determined at trial;

h. An award of pre- and post-judgment interest to the extent allowed by law;

i. A declaration that Defendants breached the TCS America Agreement; and

j. An award of such other, further, and different relief as may be just and proper in light of the circumstances of this case.

DEMAND FOR JURY TRIAL

Epic respectfully demands a trial by jury on all claims and causes of action properly tried thereto.

Dated: October ____, 2015

/s/ Nick G. Saros

Brent Caslin
bcaslin@jenner.com
Nick G. Saros
nsaros@jenner.com
Kate T. Spelman
kspelman@jenner.com
JENNER & BLOCK LLP
633 West 5th Street Suite 2600
Los Angeles, CA 90066
Tel: 213-239-5100
Fax: 213-230-5199

Anthony A. Tomaselli
aat@quarles.com
Kristin G. Noel
kristin.noel@quarles.com
Stacy A. Alexejun
stacy.alexejun@quarles.com
QUARLES & BRADY LLP
33 East Main Street, Suite 900
Madison, WI 53703
Tel.: 608.251.5000
Fax: 608.251.9166

Attorneys for Plaintiff Epic Systems Corporation

CERTIFICATE OF SERVICE

I hereby certify that on October ___, 2015, I caused a true and correct copy of the Foregoing Second Amended Complaint to be served on all counsel of record via the Court's ECF filing system.

/s/ Nick G. Saros
By: Nick G. Saros